CLAIMS

WHAT IS CLAIMED IS:

1. A system, comprising:

a processor configured to operate in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode;

one or more secured assets coupled to the processor; and

security hardware configured to control access to the secured assets dependant upon the operating mode of the processor, wherein the security hardware is configured to allow access to the secure assets in the secure operating mode.

2. The system of claim 1, wherein the secured assets comprise one or more of the group consisting of:

a random number generator,

a secure management register,

a monotonic counter, and

a secure memory.

3. The system of claim 1, wherein the security hardware comprises:

an initiation register, wherein an entry in the initiation register is an indication to change the operating mode of the processor to the secure mode.

4. The system of claim 1, wherein the secure operating mode comprises system management mode.

5. The system of claim 1, wherein the security hardware comprises:

a kick-out timer configured to provide an indication to the processor of when the processor to exit the secure mode.

6. The system of claim 5, wherein the security hardware further comprises:

a re-initiation timer configured to provide an indication to the processor to the processor to exit the secure mode into a standard mode.

7. The system of claim 1, wherein the security hardware comprises:

a duration timer configured to operate while the processor is operating in the secure mode, wherein the duration timer is configured to provide an indication of how long the processor is in the secure mode.

8. The system of claim 7, wherein the security hardware comprises:

a kick-out timer configured to provide an indication to the processor of when the processor is to exit the secure mode.

9. The system of claim 8, wherein the kick-out timer and the duration timer comprise a single timer.

10. The system of claim 8, wherein the security hardware further comprises:

a re-initiation timer configured to provide an indication to the processor to re-enter the secure mode.

11. The system of claim 1, wherein the security hardware comprises:

mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

12. The system of claim 11, wherein the input data for the one or more secured assets is addressed to the inbox of the mailbox RAM.

13. The system of claim 11, wherein the output data from the one or more secured assets is retrieved from an address at the outbox of the mailbox RAM.

14. The system of claim 11, wherein the security hardware further comprises:

access filters configured to provide input data or access requests to the inbox of the mailbox RAM if the processor is operating in the secure operating mode, wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor is not operating in the secure operating mode, and wherein the access filters are further configured to provide a predetermined response in lieu of data upon receipt of said access requests if the processor is not operating in the secure operating mode.

15. The system of claim 1, wherein the security hardware further comprises:

scratchpad RAM, wherein each of the one or more secured assets is configured to access the scratchpad RAM for the storage of data.

16. The system of claim 1, further comprising:

a memory for storing data, wherein the memory is coupled to the processor and the processor is configured to store and retrieve data from the memory in substantially all of the plurality of operating modes.

17. The system of claim 1, wherein the security hardware comprises:

access filters configured to provide access requests to one or more of the one or more secured assets when the processor is operating in the secure operating mode, wherein the access filters are further configured to provide a predetermined response in lieu of data if the processor is not operating in the secure operating mode.

18. The system of claim 17, wherein the security hardware further comprises:

access locks coupled to the access filters, wherein the access locks are configured to disable the access filters in an unlocked mode.

19. The system of claim 1, further comprising:

a battery, wherein the battery provides reserve power to the one or more secured assets.

20. The system of claim 1, further comprising:

a battery, wherein the battery provides reserve power to the security hardware.

21. A method for providing access to secured assets in a computer system, the method comprising:

switching the computer system between a first operating mode and a second operating mode, where second operating mode comprises a secure operating mode;

restricting access to the secured assets in response to the computer system being in the first operating mode; and

permitting access to the secured assets in response to the computer system being in the secure operating mode.

22. The method as set forth in claim 21, wherein the secure assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.

23. The method as set forth in claim 21, wherein the secure assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

24. The method as set forth in claim 21, wherein the secure assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

25. The method as set forth in claim 21, further comprising:

receiving a request to change the computer system from the first operating mode to the secure operating mode.

26. The method as set forth in claim 25, wherein receiving a request to change the computer system comprises providing an entry into an initiation register and asserting a control signal indicative of the entry in response to providing the entry.

27. The method as set forth in claim 26, wherein asserting the control signal indicative of the entry comprises providing a system management interrupt.

28. The method as set forth in claim 21, further comprising:

measuring a time period in which the computer system is in the secure operating mode; and

providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

29. The method as set forth in claim 28, further comprising:

measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode; and

providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time.

30. The method as set forth in claim 21, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

31. The method as set forth in claim 21, further comprising:

receiving an access request for one of the secure assets; and

wherein restricting access to the secured assets comprises responding with a predetermined response in lieu of data in response to receiving the access request for one of the secure assets.

32. The method as set forth in claim 21, further comprising:

receiving an access request for one of the secure assets; and

wherein permitting access to the secured assets comprises providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets.

33. The method as set forth in claim 21, further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets and in response to setting the access lock to the unlocked state.

34. A system, comprising:

means for switching the computer system between a first operating mode and a second operating mode, where second operating mode comprises a secure operating mode;

means for restricting access to the secured assets in response to the computer system being in the first operating mode; and

means for permitting access to the secured assets in response to the computer system being in the secure operating mode.

35. The system of claim 34, further comprising:

means for receiving a request to change the computer system from the first operating mode to the secure operating mode.

36. The system as set forth in claim 34, further comprising:

means for measuring a time period in which the computer system is in the secure operating mode; and

means for providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

37. The system as set forth in claim 34, further comprising:

means for receiving an access request for one of the secure assets; and

means for responding with a predetermined response in lieu of data in response to receiving the access request for one of the secure assets.

38. The system as set forth in claim 34, further comprising:

means for receiving an access request for one of the secure assets; and

wherein the means for permitting access to the secured assets comprise means for providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets.

39. A system, comprising:

means for processing in an operating mode, wherein the operating mode is one of a plurality of operating modes including a secure operating mode;

one or more secured means coupled to the means for processing, wherein the one or more secured means comprise one or more of the group consisting of:

means for generating a random number or nonce;

means for storing secure management data;

means for generating a monotonic value; and

means for storing secure data; and

means for controlling access to the one or more secured means dependant upon the operating mode of the processor, wherein the one or more secured means comprise means for allowing access to the secure assets in the secure operating mode.

40. A computer readable program storage device encoded with instructions that, when executed by a computer system, performs a method of providing access to secured assets in the computer system, the method comprising:

switching the computer system between a first operating mode and a second operating mode, where second operating mode comprises a secure operating mode;

restricting access to the secured assets in response to the computer system being in the first operating mode; and

permitting access to the secured assets in response to the computer system being in the secure operating mode.

41. The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a secure memory, and wherein permitting access to the secured assets comprises reading data from or writing data to the secure memory.

42. The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a random number generator, and wherein permitting access to the secured assets comprises requesting a random number from the random number generator and receiving the random number from the random number generator.

43. The computer readable program storage device as set forth in claim 40, wherein the secure assets comprise a monotonic counter, and wherein permitting access to the secured assets comprises requesting a value stored in the monotonic counter and receiving the value stored in the monotonic counter.

44. The computer readable program storage device as set forth in claim 40, the method further comprising:

receiving a request to change the computer system from the first operating mode to the secure operating mode.

45. The computer readable program storage device as set forth in claim 44, wherein receiving a request to change the computer system comprises providing an entry into an initiation register and asserting a control signal indicative of the entry in response to providing the entry.

46. The computer readable program storage device as set forth in claim 45, wherein asserting the control signal indicative of the entry comprises providing a system management interrupt.

47. The computer readable program storage device as set forth in claim 40, the method further comprising:

measuring a time period in which the computer system is in the secure operating mode; and

providing a control signal to the computer system to exit the secure operating mode in response to the time period in which the computer system is in the secure operating mode exceeding a predetermined length of time.

48. The computer readable program storage device as set forth in claim 47, the method further comprising:

measuring a time period in which the computer system is out of the secure operating mode in response to providing the control signal to the computer system to exit the secure operating mode; and

providing a control signal to the computer system to re-enter the secure operating mode in response to the time period in which the computer system is out of the secure operating mode exceeding a predetermined length of time.

49. The computer readable program storage device as set forth in claim 40, wherein permitting access to the secured assets comprises reading output data from or writing input data to a mailbox RAM from which the secure assets write the output data and read the input data.

50. The computer readable program storage device as set forth in claim 40, the method further comprising:

receiving an access request for one of the secure assets; and

wherein restricting access to the secured assets comprises responding with a predetermined response in lieu of data in response to receiving the access request for one of the secure assets.

51. The computer readable program storage device as set forth in claim 40, the method further comprising:

receiving an access request for one of the secure assets; and

wherein permitting access to the secured assets comprises providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets.

52. The computer readable program storage device as set forth in claim 40, the method further comprising:

setting an access lock to an unlocked state; and

wherein permitting access to the secured assets further comprises overriding restricting access to the secured assets and providing the access request to the one of the secure assets in response to receiving the access request for one of the secure assets and in response to setting the access lock to the unlocked state.